King County

Office of Information
Resource Management

Information Technology Governance Policies, Standards and Guidelines

Title **Vulnerability Assessment and Management Policy**	Document Code No. ITG-P06-04-1
Chief Information Officer Approval / Date 11/1/07	Effective Date.

1.0 PURPOSE:

To increase the security posture of King County and mitigate threats posed by vulnerabilities within King County system.

2.0 APPLICABILITY:

This policy applies to all King County employees, contractors, vendors and agents with access to any part of King County networks and systems. This policy applies to remote access connections used to do work on behalf of King County, including reading or sending email and viewing intranet web resources.

3.0 REFERENCES:

3.1 Enterprise Information Security Policy

3.2 King County Asset Protection Policy

3.3 Vulnerability Management and Mitigation Guidelines

3.4 Acknowledgement of Information Security Responsibilities and Confidentiality Guidelines

3.5 Patch Management Standard

3.6 RCW 42.56 (Washington Public Disclosure Act)

4.0 DEFINITIONS:

4.1 **Authenticated Scan:** A type of scan that requires appropriate credentials to authenticate to a machine to determine the presence of vulnerability with out having to attempt an Intrusive Scan.

4.2 **Information Asset:** A definable piece of information, information processing equipment, or information system, that is recognized as "valuable" to the Organization that has one or more of the following characteristics:

- Not easily replaced without cost, skill, time, or other resources;
- Part of the Organization's identity, without which the Organization may be threatened.

4.3 **Information System:** Software, hardware and interface components that work together to perform a set of business functions.

4.4 **Internal-Confidential:** The requirement to maintain certain information accessible to only those authorized to access it and those with a need to know. In this instance those authorized would only be those within King County with a designated need to know. Such documents would likely be excluded from public disclosure under RCW42.56.420.

4.5 **Intrusive Scan:** A type of scan that attempts to determine the presence of vulnerability by actively executing a known exploit.

4.6 **Network Infrastructure Equipment:** Subset of Information Assets specifically referring to equipment which provides information transport. Examples include but may not be limited to routers, switches, firewalls, bridging equipment etc. This subset usually does not include network servers and workstations unless such devices serve the specific function of providing transport.

4.7 **Organization:** Every county office, every officer, every institution, and every department, division, board and commission.

4.8 **Threat:** Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. Something or someone that can intentionally or accidentally exploit a vulnerability.

4.9 **Vulnerability:** A security exposure in an operating system or other system software or application software component. Vulnerabilities include but are not limited to missing Operating System and application Patches, inappropriately installed or active applications and services, software flaws and exploits, mis-configurations in systems, etc.

5.0 POLICIES:

5.1 **Approved Scanning Tools** – There are numerous, tools that can provide insight into the vulnerabilities on a system. Not all scanning tools have the same set of features. The Chief Information Security and Privacy Officer shall be the sole entity to implement an enterprise scanning tool. Use of any other vulnerability scanner on the KCWAN must have documented justification for use and requires approval by the Chief Information Security and Privacy Officer.

5.2 **Limitation of Scanning** – Organizations shall not conduct intrusive scans of systems that are not under their direct authority.

5.2.1 It is the responsibility of organizations to ensure that vendor equipment is free of vulnerabilities that can harm King County information assets. The vendor must be informed and permitted to have staff on hand at the time of scans. If a vendor does not provide staff, scans must be conducted to determine security status of vendor owned devices.

5.2.2 Vendors are not permitted to conduct scans of King County information assets without the express permission of the Chief Information Security and Privacy Officer and the presence of appropriate King County staff as designated by the organization.

5.2.3 At no time shall IT staff ever conduct a scan on the public network or Internet unless requested by the network owner. If such a scan is requested the Chief Information Security and Privacy Officer must be informed.

5.2.4 Information Systems that appear to be causing disruptive behavior on the network may be scanned using non-intrusive methods by impacted organizations to investigate the source of the disruption.

5.3 **Periodic Vulnerability Assessment** – Organizations will conduct a vulnerability assessment of all Information Assets on a periodic basis. The assessment will scan information assets from inside the perimeter of the KCWAN.

5.3.1 An enterprise-class vulnerability scanning and assessment tool must be used to conduct the scans (see 5.1 above). This tool must be capable of scanning information systems from a central location and be able to provide remediation suggestions. The scans must cover all information assets of the organization.

5.3.1.1 Organizations may contract external staff to complete the work however the contractors must use an enterprise-class assessment tool that provides similar capabilities as mentioned above.

5.3.1.2 If contractors are engaged to conduct scans using the King County scanning tool, approval must be obtained from the Chief Information Security and Privacy Officer.

5.3.2 Scans shall be performed during hours appropriate to the business needs of the organization and to minimize disruption to normal business functions.

5.3.3 Data from scans are to be treated as Internal-Confidential

5.3.4 The vulnerability scanning tool must have the ability to associate a severity value to each vulnerability discovered based on the relative impact of the vulnerability to the organization.

5.3.5 IT staff will not make any temporary changes to information systems, for the sole purpose of "passing" an assessment. Any attempts to tamper with results will be referred to the organizations IT management for disciplinary action. Vulnerabilities on information systems shall be mitigated and eliminated through proper analysis and repair methodologies.

5.3.6 No devices connected to the network shall be specifically configured to block vulnerability scans from authorized scanning engines.

5.3.7 At a minimum, organizations shall run authenticated scans from the enterprise class scanning tools on a quarterly basis against all information assets within their control. See Vulnerability Management and Mitigation Guidelines for suggestions on scan management.

5.4 **New Information System Vulnerability Assessment** – Organizations will conduct several vulnerability assessments of all information systems during installation and testing and prior to production operations. No new information system shall be considered in production until a vulnerability assessment has been conducted and vulnerabilities addressed.

5.4.1 A vulnerability assessment will be conducted at the completion of the operating system installation and patching phase.

5.4.2 A vulnerability assessment will be conducted at the completion of the installation of any vendor provided or in-house developed application.

5.4.3 A vulnerability assessment will be conducted just prior to moving the information system into production.

5.4.4 If an information system is provided by a vendor prior to user acceptance testing and again before moving into production vulnerability assessments must be conducted.

5.4.5 All new network infrastructure equipment must have a vulnerability assessment conducted during the "burn in" phase and prior to moving to production.

5.4.6 At the completion of each of the above vulnerability assessments all discovered vulnerabilities must be addressed with a mitigation plan developed, submitted to and approved by the Chief Information Security and Privacy Officer.

5.5 **Remediation and Compliance** – At the conclusion of each quarterly assessment each organization will produce a Mitigation and Compliance Report. This report will summarize the following:

5.5.1 List of Vulnerabilities – All discovered vulnerabilities, the severity, and the affected information systems.

5.5.2 Remediation Steps – Each vulnerability listed will have detailed information on how the vulnerability will be remedied or eliminated.

5.5.3 The report will be submitted to the Chief Information Security and Privacy Officer with a timeline for completion of remediation steps.

5.6 **Remediation Priorities** – Organizations and vendors with information assets on the KCWAN will remedy and/or mitigate discovered vulnerabilities based on the following rules.

5.6.1 "High" or "Critical" vulnerabilities will be fully addressed within 15 calendar days of discovery.

5.6.2 "Medium" level vulnerabilities will be addressed within 45 calendar days of discovery.

5.6.3 "Low" level vulnerabilities will be addressed within 180 calendar days of discovered.

5.6.4 "Informational" vulnerabilities may never be addressed.

5.7 **Remediation/Mitigation of Vulnerabilities** – If a system has a vulnerability that cannot be remediated in the recommended manner the Organization shall perform a Risk Assessment, implement **appropriate security controls to mitigate** identified risks, and provide a copy of the signed Risk Assessment to the Chief Information Security and Privacy Officer.

5.8 **Annual Report** – Organizations should generate an annual report of all outstanding vulnerabilities. This report should be submitted to the Chief Information Security and Privacy Officer for review.

5.9 **External Audit** – The Chief Information Security and Privacy Officer reserves the right to independently audit each Organization at will or at the request of the organizations management. These audits will review existing scanning data and verify that vulnerabilities were actually remediated. Any discrepancies will be noted and reported to the Chief Information Officer and the Organization's senior management.

6.0 EXCEPTIONS:

6.1 Any agency needing an exception to this policy must follow the Information Technology Policy and Standards Exception Request Process using the Policy and Standards Request form. This form can be found on the Office of Information Resource Management policies and procedures Web page at http://kcweb.metrokc.gov/oirm/policies.aspx.

7.0 RESPONSIBILITIES:

7.1 Organization management is responsible for:

- Supporting and complying with this policy.
- Reviewing reports and ensuring compliance.

7.2 IT management is responsible for:

- Supporting and complying with this policy.
- Supervising vulnerability assessments and assigning resources.
- Procuring resources to conduct the vulnerability assessments ensuring that there is no conflict of interest between assessment staff and IT staff.
- Enforcing this policy.
- Reviewing reports and assigning resources for remediation and compliance.
- Implementing policies, procedures, and practices to comply with assessment results or remediate vulnerabilities.

7.3 IT staff is responsible for:

- Supporting and complying with this policy.
- Performing remediation as directed.

7.4 Chief Information Security and Privacy Officer:

- Providing and maintaining an enterprise class vulnerability scanner to conduct scans.
- Conduct annual compliance reviews of organizations

- Assist organizations with risk assessment processes and to remediate or mitigate vulnerabilities in cases where such vulnerabilities cannot be eliminated through conventional means.
- Review quarterly and annual vulnerability reports.

7.5 Chief Information Officer:

- Is the approval authority for this policy.